22

Schengen Information System II: The balance between civil liberties, security and justice

Katina Michael[1] and MG Michael[2]

[1]Senior Lecturer, School of Information Systems and Technology, University of Wollongong, [2]Honorary Fellow, School of Information Systems and Technology, University of Wollongong

Abstract

This paper investigates the application of the Schengen Information System (SIS) in the European Union and the balance between civil liberties, security and justice. It provides an overview of the SIS, technical issues related to the maintenance of the SIS, and transnational legal issues in the context of national security and public policy. Given that citizens can now move freely between States in Europe, the paper investigates how the SIS is being administered, applied, and enforced and some of the potential problems that arise from cross mutual state recognition of SIS alerts. This paper argues that the SIS has a number of inherent and propagating weaknesses and that the risk exposure presented to citizens is far too great for the benefits that ensue. The paper recommends a movement away from the idea of a fortress Europe toward one of State to State harmonization in transnational criminal issues.

Keywords: Schengen Information System, civil liberties, security, justice

1 What is the Schengen Convention?

The Schengen Agreement was established on the 14th June 1985 when France, Germany, Belgium, Luxembourg and the Netherlands agreed to abolish

checks at their common borders, and to create a single external frontier (Council of the European Union, 1999; The European Parliament and the Council of the European Union, 1995). The actual Schengen Convention was ratified in June 1990 and came into effect in March of 1995, by which time several other States had agreed to the EU framework including Italy, Spain, Portugal, and Greece. All signatories agreed to "setting a common visa regime, improving coordination between the police, customs and the judiciary and taking additional steps to combat problems such as terrorism and organized crime" (Justice and Home Affairs, August 2005).

2 What is the Schengen Information System (SIS)?

2.1 The Schengen Information System

The Schengen Information System (SIS) was established in the Schengen Convention (Title IV) (Official Journal of the European Communities, 1999, pp. 439-459). The SIS was operational in 1995, and according to reports collapsed within 90 minutes due to system congestion (Bantekas & Nash, 2003, p. 279). The purpose of the SIS, according to Article 93 of the Convention, is to maintain "public policy and public security, including national security" (Joint Supervisory Authority, n.d.). Given that citizens can now move freely between States in Europe (ie contracting parties only), the information communicated via SIS can help ensure that provisions are met. SIS works on the basis that Member States have a National SIS (N-SIS) which is networked to a Central SIS (C-SIS) (Europa, 2007). Thus the SIS can be considered as a "series of national databases connected to a central system which holds information on suspected criminals, missing persons, unwanted aliens and stolen vehicles and documents" (Bantekas & Nash, 2003, p. 279).

> "In effect it brings together national lists of persons to be excluded from the territory of the Member States into one network, which border guards and visa officials can access online when individuals arrive at the common external border or when they ask for a visa (Guild & Bigo, 2002, p. 129)."

The data on N-SIS and the C-SIS should be identical at any given time. Transborder flows of personal data (TBFPD) are transmitted in accordance with protocols and procedures jointly established by the contracting parties. In its fundamental operation, "[t]he SIS is a database that stores criminal information from participating Member States and is considered to be the most prominent instrument of police co-operation devised under Schengen" (Bantekas & Nash, 2003, pp. 236-237). Compare the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data with the Schengen Convention (Articles

92-101) (Organisation for Economic Co-operation and Development, 1980, p. 9):

> "Data controller means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf; personal data means any information relating to an identified or identifiable individual (data subject); and transborder flows of personal data means movements of personal data across national borders."

2.2 SIS Phase II, SIRENE, Vision, and the SISNET Network

In its original phase I implementation (1995) the Schengen Information System had the capacity to serve no more than 18 participating States (Verwilghen, 2001). Given the expansion of the EU over time, the SIS would need to service more States by 2002 While most official reports identify this as the main reason of the SIS phase II, others believe that it had more to do with the States benefiting "from the latest developments in the field of information technology and to allow for the introduction of new functions" (Iocheva, 2006). It is the latter "new functions" which has concerned privacy advocates in Europe, including organizations like Statewatch (Hayes, 2005). (Hayes, 2004) is clear in his assessment of law enforcement databases, i.e. that they are a product of "original sin". He goes onto add that:

> "*[f]unction creep* is inevitable, regardless of any assurances given by the executive at the time." The notion of privacy is complex. Privacy involves the "social contract between individuals and the society which they live. It invites clashes between individuals and institutions, and between privacy protection and free access to information" (Hoffman, 1979, p. 3).

2.2.1 SIRENE

The Schengen Information System has a supplementary network, known as SIRENE (Supplementary Information Request at the National Entry). SIRENE has been described as a "network trough," and also as the "human interface" of the SIS (European Union, 2002, p. 12). By human interface, it is implied that SIRENE:

> "as a role of first-line contact both for the other SIRENEs and for the national authorities and end users. Depending on the case, SIRENE must be able to deal with it independently or to refer it to the competent authorities or agencies. SIRENE staff should therefore be

competent and well-trained and have established good contacts with national and foreign authorities."

SIRENE can exchange additional information to that included in the national portion of the SIS, as well as the C-SIS. In effect SIRENE allows smaller offices within each State to communicate with one another and act as intermediaries between national authorities responsible for the data on SIS such as judges, police and alien offices. It is important to note that the SIS Phase II network is being replaced by the SISNET network (Department of Homeland Security Public Affairs, 26 October 2006). Together these information systems can help national and local police, customs and the judiciary.

3 What information is recorded on the SIS?

3.1 Recorded categories of data

Article 94 of the Convention contains a detailed list of categories of data that can be stored in the system. The categories can be classified into three distinct types: persons, objects, and vehicles. The main objective of SIS is to exchange data on certain categories of people and lost or stolen goods. With respect to persons the following data may be stored: surnames and aliases, physical characteristics not subject to change, date and place of birth, sex, nationality, whether persons concerned are armed or violent, reason for alert, action to be taken. Articles 95-100 stipulate why an alert can be triggered by an official. The reasons include but are not limited to: arrest for the purposes of extradition, to find a missing person whose detention has been ordered, arrest for the purpose of appearing in court, discrete surveillance and specific checks (Article 99), and in the case of aliens who in most cases have not complied with provisions governing entry and residence. With respect to data stored on objects this may include: stolen motor vehicles, firearms which have been misappropriated, blank official documents which have been stolen, issues identity papers which have been stolen and suspect banknotes. While freedom of movement in the EU provides law-abiding citizens with so many benefits, criminals can also take advantage of it for the purposes of terrorism, cybercrime, drug smuggling and firearm trafficking etc. Cross-border crime is also among the most difficult to detect and contain, as several jurisdictions are involved (Justice and Home Affairs, August 2005).

3.2 Who has access to information?

Access to the information on the SIS as stated in Articles 92 and 101 of the Convention can only be by designated authorities for the purpose of border/police/custom checks carried out in the country in accordance with

national law. The primary reason for the checks is linked to varying levels of alerts, which may refuse an individual suspected of a crime entry into the designated country. There are regulations governing the type of data to be collected, the content of SIS records including responsibility for their correctness, rules on the duration of alerts, interlinking of alerts and compatibility between alerts, rules on access to SIS data, and rules on the protection of personal data and their control.

It is important to emphasize that “records” today are quite different to the flat-file databases of the past. Duncan (2004, pp. 71, 75) notes:

> “Quite unlike systems of records, today’s databases are heterogeneous. They have complex structures determined by the purposes for which they were constructed, and they are plagued by difficulties in semantic interoperability because of different vocabularies and different perspectives on the use of the data. Further they are often maintained by multiple sites, are capable of linkage of records across databases, and may not be under the control of a single authority. This makes the application of existing law and administrative procedures problematical. And yet this issue must be addressed because government databases contain highly sensitive and valuable information.”

This is particularly true of the SIS, especially given the cross-border nature of it, and the many different languages it traverses including, French, German, Italian, Greek, Finnish, Maltese etc.

4 Technical issues

4.1 The need to standardize practices

The sheer size of the SIS II and the number of Member States now in the European Union requires not only regulation but standardization in practice. “The system can be accessed from 50,000 computers by thousands of police, immigration officers and visa-issuing embassy staff” (Eaglesham, 2000). It is one thing to have a system, with policies, and procedures, and another on how these should be executed in an operational sense (Dalberg, Angelvik, Elvekrok, & Fossberg, 2006). In December 2002, the *Schengen Information System, SIRENE: Recommendations and Best Practices* manual was published so that best practices could be identified serving as “inspiration for the establishment of standards defining the minimum application of the Schengen Acquis” (European Union, 2002, p. 7). It is important to note, that after the introduction of SIS II in 2001, SIS I and SIS II were considered one and the same. Of utmost important in SIS was ensuring the balance between the number of alerts entered into the

system, and that the alerts inserted were of good quality.

> "Every national alert that is "Schengen relevant" should in principle be introduced in the SIS. However, in order to be able to execute the alert, it is necessary that the alert is correct, as complete as possible and traceable. Finally, it should be borne in mind that when a Schengen State executes an alert, it has the right to expect that the issuing Schengen State will follow up the hit. Not doing so without a valid (legal) reason will negatively impact on the willingness of (local) authorities to use the SIS and maximize its potential" (European Union, 2002, p. 11).

4.2 System maintenance, real-time updates and offline copies

A great number of technical issues abound in such a monolithic system such as the SIS that covers a great deal of Europe 'physically' and has so many people 'accessing' it and 'updating' and 'maintaining' it. Beyond the day-to-day issues of hardware and software required to operate the system 24/7, there is the need to maintain that the data shown to the end-user is in fact a true copy of the current state of affairs. For instance, it is quite possible that an alert has been changed from "high" to "low" or from "low" to "no longer valid" and this kind of change needs to be reflected in all N-SIS/C-SIS in real-time. To this end, regular automated database comparisons are required. Where on-line access to the data is not possible, regular off-line copies need to be sent and additional phone checks made. This does pose a security risk in itself- especially when it has been noted that whole databases on CD-ROM are sent regularly to Consulates (W. van de Rijt). In November of 1997, SIS data was found at a Belgian railway station accidentally left behind by an official (Eaglesham, 2000, p. 24).

4.3 Dealing with coordination issues between agencies

Coordination is a problem often cited but has been to some extent overcome by the function of SIRENE to act as a single point of contact for each Schengen State. For this matter the management structure needs to be standardized as well. Where several authorities are involved in a particular case where alerts may be conflicting, eg the Schengen State authorities and Interpol, the Schengen alerts always take precedence. In this instance, Interpol would be required to provide the Schengen State with a Schengen ID alert. Again the importance of well-trained administrative and operational staff is that they add to the robustness of the system and ensuring efficient workflow (European Union, 2002, pp. 14-15). It is also important that SIRENE offices are armed with competent legal expertise and are conversant in the appropriate languages (especially of their bordering States and of course, English).

4.4 User interface issues and data quality

From a user interface perspective, the query functionality provided by the software needs to go beyond “exact match searching” to include “phonetic queries, wildcard queries, fuzzy logic, soundex” (European Union, 2002, p. 18). Data quality of pre-existing national data on an individual should be checked for Schengen relevance and correctness before being loaded into the central SIS or into newer systems. Alerts and actions should be clearly communicated to end-users. For instance, in the case of misused identity, the procedure to deal with a given *hit* and the subsequent investigations required should make it known whether the individual in question is the victim of identity fraud, or the perpetrator of the misuse. Consider the case where an Ethiopian citizen living in Budapest who was refused admission to France because his name was entered on the SIS in Germany after he reported a missing passport. It took eight months to get the information corrected (Eaglesham, 2000).

4.5 Data handling issues and alerts

Beyond data quality is the issue of data handling. In the event an alert is recorded, it should satisfy the criteria of the Schengen Convention in accordance to Article 95, to ensure a *hit* will be followed up. If an alert is identified as invalid, SIRENE operators should have the capability to delete it. In the same token, when an alert is extended, its on-going validity should be re-examined, and a reply to that given case should be provided in the shortest possible time. For instance, when one Schengen State alerts another Schengen State of a positive response on a given alert, it is a *hit*, and these should also be recorded. Each alert should have a separate Schengen ID number allotted to it to ensure that audits of events are possible and also to minimize confusion between the States. Operators should not fill in mandatory fields with words like “unknown” as this renders untraceable information, in the same token it is important that operators act ethically to ensure that they are not documenting things that are not reflective of evidence.

4.6 The growing need for security policies

All these technical issues do lend themselves to a security policy which is standardized across all of the Schengen information technology (IT) systems. Who has access to these systems, at what appropriate level and for how long, is something that is not easy to solve. Indeed this is one of the major problems identified by experts regarding monolithic systems such as the SIS. There are no easy answers to this issue, only to ensure that SIRENE recruit responsible personnel with the appropriate clearance and certification. In terms of physical security, the SIS has computers located underground, differing security zones,

staff use access cards for entry, there are armed-guards and closed circuit television monitoring (CCTV) at entries and exits (European Union, 2002, p. 30). Staff also have unique IDs and passwords to log onto the systems securely.

5 Legal issues

5.1 Cross mutual recognition versus harmonization

The SIS is fraught with well-known legal issues. According to Minas Samatas (2003, p. 141):

> "[t]he more serious implementation problems of the SIS are the legal ones – regarding the protection of citizens' privacy and civil liberties, as well as the human rights of foreigners."

At the first instance, the SIS is populated by individual Schengen States according to a national understanding of the criteria for inclusion and a national interpretation of public order and security. "The underlying principle of the system is based on the notion of cross mutual recognition of national decisions rather than harmonization" (Guild & Bigo, 2002, p. 126). For instance, if a person is deemed to have acted inappropriately in one Member State and their personal data is subsequently recorded in the SIS (while the individual is still in that territory), then other Member States need to act upon that 'alert'. However, what one Member State deems a "risk", another Member State may not, yet they are still bound to the Schengen Convention.

What is perceived as a security risk in one state is not necessarily the same in another. This difference of perception of the notion within the Union will be the territory where national courts begin to question the legitimacy of the system (Guild & Bigo, 2002, p. 129).

5.2 The Visa List and profiling for potential criminals

Many legal representatives across the globe see another fundamental error with the SIS- it not only is used for outright 'exclusion' of an individual from the EU based on one Member State's understanding of the criteria, but it also can identify 'groups' of persons who supposedly pose a greater risk to the EU based on their nationality as depicted on the 'visa list' (Harper, 2006). It should be highlighted that these are individuals who have done nothing wrong, have been in an EU Member territory for some time, and who would have otherwise been entitled to freedom of movement within the EU exterior border, but who for the fact that they have been born in a particular country, are categorized as being 'more' or 'less' likely to be a risk (Guild & Bigo, 2002, p. 127). By controlling the individual through a visa requirement, jurisdictional issues are placed back in the hands of the individual's own State (Department of Homeland Security Public

Affairs, 2006). Profiling techniques are used on these groups, and individuals anticipated to be 'a criminal' (or who may become a criminal over time) are excluded (Strandburg & Raicu, 2006). There are fundamental problems with this- who actually defines what constitutes a risk to security? It should also be noted that until the mid-1980s visas were regarded as "expressions of mistrust", especially of non-EU migrants (Anderson & Apap, 2002, p. 247).

5.3 Human rights versus a 'Fortress Europe'

If the basis for what information can be entered into the SIS is national law, then a National-SIS (N-SIS) may make complete sense, but a patchwork of national lists brought together in a Central-SIS (C-SIS) may not.

> "This means by which the authorities of a Member State come to the decision to enter the data are under the exclusive control of the Member State authorities. Thus a Member State could have other reasons than security to include a person on the list and this would not breach Article 96… There is no attempt to restrict or harmonize what is permissible at the national level. But whatever happens at that level is then to be recognized as value by the other States" (Guild & Bigo, 2002, p. 131).

To illustrate this point, consider the number of records in the central SIS as of May 23, 2000 was 9.7 million. The country with the most entries about persons was Germany. During this period, there was a perceived threat to Germany by 'foreigners' which constituted both asylum seekers, and ethnic Germans from Central and Eastern Europe (known as *Aussielder*). This caused quite a bit of public disquiet to the measure that asylum seekers, now considered outright foreigners, were entered into the SIS because they were seen as a "risk category". France on the other hand, at the time, had a different view on asylum but still had to reject the persons who had been inserted into the SIS. This kind of perceived misuse of the SIS is in direct conflict with the obligation of Member States to "provide protection to persons fearing persecution and torture" (Guild & Bigo, 2002, p. 134).

6 Transnational issues

When considering a system like the Central Schengen Information System, by its very nature, it poses transnational challenges (House of Lords, 2007). It is an information system that traverses a great number of national borders and therefore jurisdictions, and as a result is subject to harmonization problems. At the heart of the problem is the principle of equality of treatment, human rights, and the function of the State within the context of the EU ((Electronic Privacy Information Centre & Privacy International, 2003, p. 59). According to (Samatas,

2003, p. 141): “[i]t is clearly an ‘immigration anathema’ to build a ‘Fortress Europe’, especially as regards Third World immigrants’ and refugees’ rights and life chances in the EU.”

‘Security’ and ‘risk’ will always mean different things to each Member State, and no amount of ‘best practice’ literature will ever eradicate this issue. While in theory the C-SIS can help to facilitate and minimize crime in the EU, by increasing cooperation and knowledge sharing between Member States and respective authorities down to the local level, it sends conflicting messages regarding principles and standards documented in the European Convention on Human Rights and within an international law context. This type of *Europeanization* may also end up contributing to the erosion of national sovereignty (Boer, 2002, p. 152).

7 Freedom, security and justice in the EU

There is no doubt that the European Union has tried to provide internal security for its law-abiding citizens, to move freely between Member States, and to enjoy the stability, wealth and internal liberal environment. Ironically, however this requirement to ensure ‘security’ has come at the expense of ‘freedom’; with the erosion of freedom has also come the problem of ‘justice’. This means that a greater balance must be struck between opposing forces which are at play. Monar (2002, p. 167) cite one example of this balance needing to be struck with the

> “EU measures in the fight against cross-border crime and illegal immigration, which now involves a range of major EU-wide data-bases, [and which] must respect high standards in terms of the protection of personal data and comply with strict rules on the interception of telecommunications and other investigative techniques…”

If the protection of personal data is not maintained appropriately, for instance in the quite plausible scenario that persons may accidentally or deliberately (Fijnaut, 2002, p. 219) be named on the C-SIS by a Member State when they are in actual fact innocent of any crime, then there is clearly a fundamental erosion of human rights at play.

> “For Euro-skeptics and human rights activists, on the other hand, a serious concern over the SIS is whether its function will diminish the protection of civil liberties and human rights in countries like Greece, which have an authoritarian state culture and a rather negative historical record on human rights” (Samatas, 2003, p. 147).

The reality is that there can never be a balance between freedom, security and justice where these types of monolithic information systems exist. While

freedom has to do with an individual's 'privacy' (ie autonomy, self-possession, integrity) (Garfinkel, 2000, p. 5), 'security' has to do primarily with the State, and justice is supposed to ensure some kind of balance. The bigger these systems get, the more potential there is for error, especially given the nature of transborder personal data flows. This does not negate of course, the obvious benefits that these systems have contributed, especially for law enforcement agencies in the tracking of stolen vehicles and other like objects but these benefits do not in themselves remove the deep-rooted problems pertaining to data quality, data correctness, breaches in personal privacy, access to information in the SIS II and beyond.[1] While it is the role of the Joint Supervisory Authority (JSA) on Schengen to maintain data protection of the SIS and new emerging networks, they are there only within a supervisory capacity with little 'authority' to enact change (Joint Supervisory Authority, 2004, June 2005; Secretariat, 2007). There is here a concluding call for more protective mechanisms and access controls[2] to be put in place, including technical regulations which are binding to Member States, beyond guidelines.[3]

References

Anderson, M., & Apap, J. (2002). *Police and Justice Co-operation and the New European Borders*. London: Kluwer Law International.

Bantekas, I., & Nash, S. (2003). *International Criminal Law*. London: Cavendish.

Bassiouni, M. C. (2003). *Introduction to International Criminal Law*. New York: Transnational Publishers.

Boer, M. D. (2002). Intelligence Exchange and the Control of Organised Crime. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and The New European Borders* (pp. 151-161). The Hague: Kluwer Law International.

[1] The debate between an individual's privacy and the security of the state continues. According to (Crosbie, 2006): 'We never get any evaluations on the effectiveness or a data-privacy cost-benefit analysis. But if you oppose this you are said to be soft on terrorism and you are endangering the fight on terrorism.' The effectiveness of the system in terms of 'hit' rate (ie alert, action, response) is also under question. See also (Bantekas & Nash, 2003) p. 280: 'The successful 'hit rate' of the system is generally low and it is questionable whether the information held on the SIS is accurate. The data protection provisions of this system, which holds approximately 9.7 million files, have been subjected to severe criticism.'

[2] 'In addition to avoiding formal procedures, prosecuting authorities engage in informal mutual co-operation practices by simply allowing police officers in another jurisdiction access to evidence' (Bantekas & Nash, 2003) p. 259. At present it is this informal cooperation which needs to be formalized.

[3] 'In the last few decades, law enforcement and intelligence cooperation has significantly increased. They are an important form of international cooperation… [but] there are no treaties applicable to law enforcement and intelligence cooperation… nor are there such forms of information-gathering and information-sharing by and between different agencies within separate countries. Regrettably, this important form of international cooperation has not yet been included in mutual legal assistance treaties. Consequently, there are no legal or judicial safeguards to insure effective and regulated modalities of information-gathering and information-sharing between intelligence, law enforcement, and prosecutorial agencies. Thus effectiveness is reduced and potential abuses are increased. This affects the accuracy of the information, and can lead to undue invasion of privacy. Because these practices are internationally unregulated, and nationally unmonitored by the judiciary when committed other than on the national territory, they pose a challenge to due process of law and to the right of privacy' (Bassiouni, 2003), pp. 368-369.

Council of the European Union. (1999). *8415/99 Limite Schengen 52*.
Crosbie, J. (2006). EU regulations: MEPs seek to restrict police access to visa data. *The Economist Intelligence Unit Ltd*.
Dalberg, V., Angelvik, E., Elvekrok, D. R., & Fossberg, A. K. (2006). *Cross-cultural Collaboration in ICT Procurement* Paper presented at the Proceedings of the 2006 International Workshop on Global Software Development for the Practitioner Shanghai, China.
Department of Homeland Security Public Affairs. (26 October 2006). The United States Mission to the European Union. Retrieved 9 October 2007, from http://www.useu.usmission.gov/Dossiers/Travel_Documents/Oct2606_ePassport_VWP.asp
Department of Homeland Security Public Affairs. (2006). The United States Mission to the European Union. 26 October. Retrieved 9 October 2007, from http://www.useu.usmission.gov/Dossiers/Travel_Documents/Oct2606_ePassport_VWP.asp
Duncan, G. T. (2004). Exploring the Tension Between Privacy and the Social Benefits of Government Databases. In P. M. Shane, J. Podesta & R. C. Leone (Eds.), *A Little Knowledge: Privacy, Security, and Public Information after September 11* (pp. 71-88). New York: The Century Foundation Press.
Eaglesham, J. (2000). EU's Largest Database 'Contains Serious Flaws' Human Rights Pressure Groups Call for Inquiry. *Financial Times*.
Electronic Privacy Information Centre, & Privacy International. (2003). *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments*. New York: EPIC, PI.
Europa. (2007). Member States of the EU. Retrieved 12 October 2007, from http://europa.eu/abc/european_countries/index_en.htm
European Union. (2002). *Volume 2: Schengen Information System: SIRENE: Recommendation and Best Practices*.
Fijnaut, C. (2002). The Problem of Corruption of Police Officials. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and the New European Borders* (pp. 219-226). The Hague: Kluwer Law International.
Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. Beijing: O'Reilly.
Guild, E., & Bigo, D. (2002). The Schengen Border System and Enlargement. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and the New European Borders* (pp. 121-138). The Hague: Kluwer Law International.
Harper, J. (2006). *Identity Crisis: How Identification is Overused and Misunderstood*. Washington: CATO Institute.
Hayes, B. (2004). From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained. Retrieved 29 May 2007, 2007
Hayes, B. (2005). SIS II: Fait Accompli? Construction of EU's Big Brother Database Underway. Retrieved 28 May 2007, 2007, from http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf
Hoffman, L. J. (1979). A Research Agenda for Privacy in the Next Decade. In L. J. Hoffman (Ed.), *Computers and Privacy in the Next Decade* (pp. 3-6). Sydney: Academic Press.
House of Lords. (2007). *Schengen Information System II (SIS II): Report with Evidence (9th Report of Session 2006-07)*. London: The Stationary Office Limited.
Iocheva, M. (2006). European Parliament Backs Compromise to Extend Schengen Information System to New Member States. *US Fed News Services*.
Joint Supervisory Authority. (2004). Opinion on the Development of the SIS II. Retrieved 11 October 2007, from http://www.cnpd.pt/bin/actividade/SISII_opinion.pdf

Joint Supervisory Authority. (June 2005). ARTICLE 96 INSPECTION: Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System. Retrieved 11 October 2007, from http://www.statewatch.org/news/2005/sep/jsa-sis-art96-rep.pdf

Joint Supervisory Authority. (n.d.). The Schengen Information System. Retrieved 17 September 2007, from http://www.garanteprivacy.it/garante/navig/schengen/jsp/main.jsp?

Justice and Home Affairs. (August 2005). Schengen Convention: Abolition of Internal Borders and Creation of a Single EU External Frontier. Retrieved 11 October 2007, from http://ec.europa.eu/justice_home/fsj/freetravel/frontiers/wai/fsj_freetravel_schengen_en.htm

Monar, J. (2002). The Problems of Balance in EU Justice and Home Affairs and the Impact of 11 September. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and the New European Borders* (pp. 165-182). The Hague: Kluwer Law International.

Official Journal of the European Communities. (1999). *The Schengen Acquis*.

Organisation for Economic Co-operation and Development. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD.

Samatas, M. (2003). Greece in 'Schengenland': blessing or anathema for citizens' and foreigners' rights? . *Journal of Ethnic and Migration Studies, 29*(1), 141-156.

Secretariat, D. P. (2007). The Joint Supervisory Authority of Schengen Retrieved 10 October 2007, from http://www.schengen-jsa.dataprotection.org/

Strandburg, K., & Raicu, D. S. (2006). *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. New York: Springer.

The European Parliament and the Council of the European Union. (1995). *Protocol Integrating the Schengen Acquis in the Framework of the European Union*.

Verwilghen, M. (2001). *Council Regulation (EC) No 2424/2001 of 6 December 2001 on the Development of the Second Generation Schengen Information System (SIS II)*: Official Journal of the European Communities.

W. van de Rijt. (7-8 December 2000). *Council of the European Union.* Paper presented at the ERA Seminar: Schengen in the Nordic States, Helsinki.